【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】平成30年11月22日(2018.11.22)

【公表番号】特表2018-501680(P2018-501680A)
【公表日】平成30年1月18日(2018.1.18)
【年通号数】公開・登録公報2018-002
【出願番号】特願2017-519901(P2017-519901)
【国際特許分類】
Ｈ０４Ｌ　9/32　(2006.01)
Ｇ０６Ｑ　20/32　(2012.01)
Ｇ０６Ｑ　20/38　(2012.01)
Ｇ０６Ｆ　21/31　(2013.01)
Ｇ０６Ｆ　21/62　(2013.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６７３Ｃ
Ｇ０６Ｑ　20/32　３３０
Ｇ０６Ｑ　20/38　３１６
Ｇ０６Ｆ　21/31
Ｇ０６Ｆ　21/62　３０９

【手続補正書】
【提出日】平成30年10月12日(2018.10.12)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
近距離無線通信能力を有するデバイスに関連する方法であって、該方法は、以下：
デバイスによって、ユーザによって入力されたパスワードを受信することであって、ここでパスワードは、パスワードのユーザ入力の前にはデバイスに記憶されていない、前記受信すること、
ユーザ入力パスワードの機能として暗号化キーを発行すること、ここでユーザ入力パスワードは、暗号化されたトークンを発行した後にデバイスに記憶されていない、
暗号化キーを使用して暗号化されたトークンを解読すること、
トークンが正しく解読されたかどうかを検証すること；
トークンが正しく解読されたことの検証に応答して、暗号化キーを使用してクレデンシャルを解読すること；および
解読されたクレデンシャルを使用して、リーダとの近距離無線通信取引を開始すること、
を含む、前記方法。
【請求項２】
暗号化キーを発行することが、１以上のデバイス特定の値の追加的な機能である、請求項１に記載の方法。
【請求項３】
暗号化キーを発行することが、ユーザ生体認証データ、スライダ値、反復カウンタ値、初期化ベクタ、およびソルトを含む群から選択される１以上のキー発行パラメータの追加的な機能である、請求項２に記載の方法。

【請求項４】
暗号化キーを使用してトークンを暗号化して暗号化トークンを形成することをさらに含む、請求項３に記載の方法。
【請求項５】
データバイトのＮｘＭ行列を回転させることによってトークンを生成すること、ここで、ＮおよびＭは非ゼロの正の整数であり；回転させたＮｘＭ行列における各バイトに排他的ＯＲを適用すること；および、回転させたＸＯＲのＮｘＭ行列をアレイ中に変換することをさらに含む、請求項４に記載の方法。
【請求項６】
巡回冗長検査、ＬＵＨＮ検査、および短い暗号文からなる群から選択される１以上の自己承認技術を使用して、データバイトのＮｘＭ行列を承認することをさらに含む、請求項５に記載の方法。
【請求項７】
暗号化されたトークンを暗号化された手法で記憶することをさらに含む、請求項６に記載の方法。
【請求項８】
暗号化キーを発行することが、ユーザ生体認証データ、スライダ値、反復カウンタ値、初期化ベクタ、およびソルトを含む群から選択される１以上のキー発行パラメータの追加的な機能である、請求項１に記載の方法。
【請求項９】
スライダ値が、サイトキーの所定の位置に窓関数を適用することで生成される、請求項８に記載の方法。
【請求項１０】
システムであって：
少なくともの１つのプロセッサ；および、
コンピュータ可読命令を記憶する少なくとも１つのメモリを含み、該命令は、少なくとも１つのプロセッサで実行されると、システムに：
ユーザ入力パスワードを受信させ、ここでパスワードは、パスワードのユーザ入力の前にはデバイスに記憶されておらず；
パスワードに基づいて暗号化キーを発行させ、ここでユーザ入力パスワードは、暗号化キーを発行した後にシステムに記憶されていない；
暗号化キーを使用してトークンを解読させ；
トークンが正しく解読されたことの検証に応じて、暗号化キーを使用してクレデンシャルを解読させ；および、
解読されたクレデンシャルを使用して、リーダとの近距離無線通信取引を開始させる、前記システム。
【請求項１１】
コンピュータ可読命令を記憶する少なくとも１つのメモリが、少なくとも１つのプロセッサで実行されたときに、システムに、さらに１以上のデバイス特定の値に基づいて追加的に暗号化キーを発行させる、請求項１０に記載のシステム。
【請求項１２】
コンピュータ可読命令を記憶する少なくとも１つのメモリが、少なくとも１つのプロセッサで実行されたときに、システムに、ユーザ生体認証データ、スライダ値、反復カウンタ値、初期化ベクタ、およびソルトを含む群から選択される１以上のキー発行パラメータに基づいて追加的に暗号化キーを発行させる、請求項１１に記載のシステム。
【請求項１３】
コンピュータ可読命令を記憶する少なくとも１つのメモリが、少なくとも１つのプロセッサで実行されたときに、システムに、さらにデータバイトのＮｘＭ行列を回転させ、ここで、ＮおよびＭは非ゼロの正の整数であり；回転させたＮｘＭ行列における各バイトに排他的ＯＲを適用させ；および、回転させたＸＯＲのＮｘＭ行列をアレイ中に変換させる

ことによってトークンを生成させる、請求項１２に記載のシステム。
【請求項１４】
コンピュータ可読命令を記憶する少なくとも１つのメモリが、少なくとも１つのプロセッサで実行されたときに、システムに、さらに巡回冗長検査、ＬＵＨＮ検査、および短い暗号文からなる群から選択される１以上の自己承認技術を使用して、データバイトのＮｘＭ行列を承認させる、請求項１３に記載のシステム。
【請求項１５】
コンピュータ可読命令を記憶する少なくとも１つのメモリが、少なくとも１つのプロセッサで実行されたときに、システムに、さらに暗号化されたトークンを暗号化された手法で記憶させる、請求項１４に記載のシステム。